UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/769,104	01/30/2004	Catalin D. Sandu	307660.01	9006

47973 7590 08/18/2009
WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER	
HAILU, TESHOME	
ART UNIT	PAPER NUMBER
2434	
MAIL DATE	DELIVERY MODE
08/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/769,104	**Applicant(s)** SANDU ET AL.
	Examiner TESHOME HAILU	**Art Unit** 2434

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2008 and 15 April 2009*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,9,10,13 and 17* is/are rejected.

7)☒ Claim(s) *7-8, 11-12, 14-16, 18-20* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on December 22, 2008 and an election filed on May 21, 2009. Claims 1-20 have been amended and elected.

2. Claims 21-22 have been canceled.

3. Claims 1-20 are pending.

Election/Restrictions

4. Applicant's representative has responded to the restriction requirement sent on April 15, 2009 by cancelling claims 21 and 22 (inventions listed as group II); and therefore, claims 1-20 (invention listed as group I) are pending; and are examined.

Response to Amendment

5. Applicant's arguments filed on December 22, 2009, with respect to claims 1-20 have been fully considered but they are moot in view of new ground(s) of rejection.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-6, 9-10, 13 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hursey et al (Hursey) (US Pub. No. 2003/0074573) in view of Marwaha (US Pub. No. 2004/0181685).

As per claim 1 Hursey discloses:

A computer-implemented malware detection system for determining whether an executable script is malware according to its functionality, the malware detection system comprising: (page 1, paragraph 2, this invention relates to the field of data processing systems. More particularly, this invention relates to scanning for malware, such as, for example, computer viruses, Trojans, worms, banned files and banned words within e-mail messages).

A malware signature store including at least one known malware script signature, wherein each malware signature in the malware signature store is a normalized signature of a known malware script; (page 2, paragraph 22, the anti-virus scanning system 8 incorporates the virus definitions 12 in the form of uncompressed virus signatures (malware signatures) 17. These virus signatures 17 might typically correspond to a sequence of twenty or so byte values that are indicative of a particular piece of malware. These uncompressed virus signatures 17 may be compressed using the coding table from the compressed computer file 16 to yield compressed virus signatures 18) and (page 2, paragraph 28, It would also be possible to compress all the uncompressed virus signatures as one task and then use this library of compressed virus signatures to search the compressed computer file).

Wherein the malware detection system is configured to: compare the normalized signature of tile executable script to the at least one normalized malware signature in the malware signature store to determine whether the executable script is malware; (abstract, line 1-6, A malware scanner (8) operates to scan compressed computer files (16) by compressing the malware signatures (17) using the same compression algorithm as used for the compressed computer file and then comparing the compressed malware signatures (18) with the compressed computer file directly). According to Hursey, the signature of known virus is compressed in order to change the signature to a common format as the incoming compressed computer files.

Report whether the executable script is malware according to the determination. (Page 2, paragraph 26, Step 38 determines whether or not a match has occurred between the compressed virus signature and the compressed computer file. If a match has occurred, then the anti-virus actions are triggered at step 40. These anti-virus actions may include deletion, quarantine, repair, alert message generation etc).

A normalization module that obtains an executable script and generates a normalized signature for the executable script, wherein generating a normalized signature for the executable script comprises translating tokens from the executable script into normalized tokens conforming to a common format; (abstract, line 1-6, A malware scanner (8) operates to scan compressed computer files (16) by compressing the malware signatures (17) using the same compression algorithm as used for the compressed computer file and then comparing the compressed malware signatures (18) with the compressed computer file directly).

Hursey does not explicitly disclose about normalization module. However, in the same field of endeavor, Marwaha teach this limitation as, (page 12, paragraph 142, at 1102, the message is normalized for example, by extracting necessary information from the message and formatted into a standard format or a token. An index is also assigned to the standardized token. At 1106, additional information is added to the standardized token) and (abstract, line 1-4, a common event format associated with unique index value is provided to allow a common structure to rules, regardless of from which system the message is originating. Messages coming from different sources into an enterprise manager are tokenized to contain essential information, and standardized into a common event format).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Hursey and include the normalization module using the teaching of Marwaha in order to standardized the incoming data from various source and generate a normalized data in a common format.

Claims 3, 4 and 5 are rejected under the same reason set forth in rejection of claim 1:

As per claim 2 Hursey in view of Marwaha discloses:

The malware detection system of Claim 1, further comprising a comparison module, wherein the comparison module compares the normalized signature of the executable script to the at least one normalized malware signature in the malware signature store. (abstract, line 1-6, A malware scanner (8) operates to scan compressed computer files (16) by compressing the malware signatures (17) using the same compression algorithm as used for the compressed computer file and then comparing the compressed malware signatures (18) with the compressed computer file directly).

Claims 10, 13 and 17 are rejected under the same reason set forth in rejection of claim 2:

As per claim 6 Hursey in view of Marwaha discloses:

The malware detection system of Claim2, wherein translating tokens from the executable script into a common format suitable for comparison with the at least one malware signature in the malware signature store comprises renaming tokens from the executable script according to a common naming convention. (Page 2, paragraph 22, the anti-virus scanning system 8 incorporates the virus definitions 12 in the form of uncompressed virus signatures (malware signatures) 17. These virus signatures 17 might typically correspond to a sequence of twenty or so byte values that are indicative of a particular piece of malware. These uncompressed virus signatures 17 may be compressed using the coding table from the compressed computer file 16 to yield compressed virus signatures 18).

As per claim 9 Hursey in view of Marwaha discloses:

The malware detection system of Claim 6, wherein generating a normalized signature for the executable script further comprises generating a set of normalized tokens for each routine in the executable script. (Abstract, line 1-6, A malware scanner (8) operates to scan compressed computer files (16) by compressing the malware signatures (17) using the same compression algorithm as used for the compressed computer file and then comparing the compressed malware signatures (18) with the compressed computer file directly).

Allowable Subject Matter

8. Claims 7-8, 11-12, 14-16, 18-20 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TESHOME HAILU whose telephone number is (571)270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Teshome Hailu/

Examiner, Art Unit 2434

/Michael J Simitoski/
Primary Examiner, Art Unit 2439